5. INFORMATION AND CYBER OPERATIONS

[Related topics: 2.7, 2.11, 2.17, 2.23, 4.1]

HIGHEST PRIORITY TOPICS FOR FY 09 (5.1 THROUGH 5.50

5.1 Cyber Conflict

- What constitutes a cyber attack?
- Appropriate responses to a cyber attack? Ladder of escalation? Horizontal escalation options?
- What are the law and policy issues that need to be addressed for the conduct of cyber warfare?
- What are the USAF rules of engagement in the event of a cyber conflict?
- What existing criminal law, rules, and regulations pertain to cyber warfare?
- What are the international norms for cyber attacks?
    - Do we need to create an ICAO equivalent for the cyber realm?
    - Can we or should we attempt to shape the cyber environment?
    - What are the analogies for surface, air, and space, sovereignty, and norms, etc?
    - What is the attribution?

POC: INSS 719-333-2717/DSN: 333-2717
Priority: 1a
Key Terms: Information Operations, law, policy.

5.2 How does the US engage the constructive Muslim Ummah to counter violent extremist Ideology?

- What are the barriers to the flow of information among 10-40 year old Muslims (focus primarily on Saudi Arabia, Egypt, Yemen, Algeria, Pakistan and in Europe)
- What can the USG do to reduce these barriers?
- What USG policies and/or actions should be increased, strengthened and/or reduced to enhance positive engagement of the constructive Muslim Ummah?

POC: Mr Andrew Simanski USSOCOM J239 210-977-2648/DSN 969-2136
Priority: 1a
Key Terms: Influence, ideology, public affairs, media,

5. 3 What is the Air Force plan in the event of "net down" operations?

- What are the contingency plans for continuing aerospace operations after losing network connectivity?

POC: Lt. Col Peter A. Garretson HQ USAF/A8XC 703-428-0891/DSN 328-0891
Dr. Cain, AWC, 334-953-1028
Priority: 1
Key Terms: IO, IW, PSYOP, JPOTF, Commando Solo, education.

5.4 Electronic Warfare Capabilities

- What are the USAF options for developing or adapting a new EW platform?
- Future of Joint USAF/USN EA-6B operations?
- Is this still a USAF priority?
- How late is too late to recapitalize the capability?

POC: Lt. Col Young 360-257-3567/DSN 820-3567
Priority: 1
Key Terms: EW, EF-111, EA-6B.

5.5 What could be the DOD role in protecting cyberspace for the United States?

- Summarize existing national and DOD guidance (e.g. PDDs, national plans, DOD directives).
- Conduct a deficit analysis between infrastructure threats and existing protection programs.
- Analyze possible new approaches to protection of the national infrastructure, and how to address the threat.
- What are the legal and ethical limits that must be taken into consideration?

POC: Dr. Kuehl, NDU, Comm 202-685-2257
Priority: 1
Key Terms: IO, IW, NII, Defending America's Cyberspace, Homeland Defense

OTHER TOPICS GROUPED BY PRIORITY

5.6 Analyze netcentric capabilities.

- How is the DOD conducting netcentric operations?
- How are networks used in current operations?
- What are the operational impacts of information sharing?
- How can netcentric operations be improved in a coalition environment?
- Discuss the balance of information security and the needs of the warfighter.
- Identify Centers of Gravity and conduct a dependency analysis for cyberspace
- Examine interdependencies within a network that are key to netcentric
    - operations
- How is adaptability and reconfigurability of communications equipment relevant to flexible command and control?
- What is the benefit and risk of wireless networks?

POC: Dr. Kuehl, NDU, 202-685-2257
Priority: 1
Key Terms: COG, netcentricity, network relationships, key nodes, interoperability

5.7 What unintended consequences (or "blowback") could result from the employment of offensive cyber on information operations?

- Would the purported deniability or non-traceability of electronic attacks prevent attacked societies from focusing on the originating country or group?
- Just as traditional US military capabilities have shown a clear progression away

from mass effects against societies and toward precision effects against military capabilities, should IW policy and capabilities, if/when developed, focus on precision rather than mass information effects?

- What is the effect of large-scale offensive cyber operations that address civilian infrastructure and defense issues? What are the policy issues associated with these various scenarios?
- How does the unpredictability of the "weapon" create law of armed conflict (LOAC) issues?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key Terms: IO, IW, LOAC, law of armed conflict, unintended consequences, policy issues, Computer Network Operations, blowback

5.8 What are the implications of international treaties and agreements in the IW realm?

- Article 5 of the North Atlantic Treaty says that "an armed attack against one or more of them in Europe or North America shall be considered an attack against them all." How does this relate to cyber attacks?
- How would an equitable arms control agreement be defined? What benefits might accrue? How are USAF equities protected?
- How are other IW powers' technological advances anticipated and addressed?
- What arms control mechanism(s) and forum would be most appropriate for
    - IW arms control? Is it possible to track/identify foreign IO/IW technology
    - capabilities?
- How would the US Government identify, vet, and publish such a foreign "IW Militarily Critical Technologies List?" Given the short life cycle and rapid evolution of IO technologies, is this feasible given the existing bureaucratic processes?
- Is there a need for Cyber Arms Control Treaties? Will they benefit the US or constrain US capabilities

POC: INSS, 719-333-2717/DSN 333-2717, Dr. Kuehl, NDU. 202-685-2257
Priority: 1
Key Terms: IO, IW, arms control, CNA, CND, IW agreements, critical technologies, proliferation

5.9 How do we measure nation-states'/non-state entities' levels of vulnerability to IO?

- Does the US do too much "mirror-imaging"? What models can be used to avoid errors made my mirror-imaging?
- Examine portions of a potential adversary's infrastructure. Include insights on why categories were chosen, application to other analysis, and potential interrelationships between categories.
- How do we determine the key nodes/centers of gravity (COGs) in an adversary's information infrastructure? What models are useful in determining nodes/COGs for Influence Operations?
- Compare and contrast kinetic and non-kinetic effects.

- Discuss how different states or cultures receive information.

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key Terms: IO, IW, vulnerability, mirror imaging, infrastructure, COG, targeting, Influence Operations

5.10 Fatwas against Extremism – How do we engage the constructive Muslim Ummah to counter violent extremist ideology?

- What fatwas against extremism have been issued, by whom, and from what region of the world?
- What response did the fatwas provoke from violent extremist organizations?
- Were the fatwas effective to dissuade individuals from joining extremist groups or pursuing jihad?
- What segments of the populations were the fatwas effective or ineffective?
- How can planners further disseminate the messages of the fatwas?

POC: Mr Andrew Simanski USSOCOM J239, 210-977-2648/DSN 969-2136
Priority: 1
Key Terms: Influence, ideology, public affairs, media

5.11 How can US Public Diplomacy Efforts be synchronized to undermine the ideological foundations of terrorism?

- How can US Public Diplomacy efforts be synchronized in order to best undermine the ideological foundations of terrorism?
- How can US Public Diplomacy efforts help empower partner nations, the constructive Muslim Ummah and their leaders to reject violent extremist ideology>
- How can US Public Diplomacy reinforce what is commonly believed by the majority of Muslims, and their religious and government leaders that terrorism is illegitimated, violates a country's sovereignty and carries a high social cost?

POC: Mr Andrew Simanski USSOCOM J239, 210-977-2648/DSN 969-2136
Priority: 1
Key Terms: Influence, ideology, public affairs, media

5.12 What is the effect of international media on US military operations and on IW/IO planning?

- Citing case studies as examples, discuss which IW/IO means were most important for a given side in a particular conflict.
- How should the AF and DOD provide international public information?
- What is the effect on the US military actions by not using the international media or having an implemented global communications strategy?
- How can IW/IO planning better involve the international media?
- What is the relationship between strategic communications and IO?
- Describe ways the US might respond to propaganda and hostile media.

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 1
Key Terms: IO, IW, media, IO planning, Kosovo, Serbia, Afghanistan, Iraq

5.13 What are measures of effectiveness (MOEs) for IW, or one of its disciplines?

- What are ways to measure IW contributions in terms of denying data, information, knowledge, understanding, and operational wisdom? How can this be related to achieving the commander's objective?
- How can the Unified Joint Task List (UJTL) MOEs be used as a foundation for more sophisticated MOE development?
- Can Joint Munitions Effectiveness Manuals (JMEMs) be developed for IW?
- What do commanders expect of IW and how can those expectations be measured?
- How can IW MOEs be validated?
- What are some MOE categories (e.g., planning process, programmatic, logistical, time, damage, perception management, etc.)?
- What are ways to conduct IW combat assessment (like battle damage assessment)?
- How do difficulties in developing MOE impact the willingness to utilize IO tools?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 2
Key Terms: IO, IW, measures of effectiveness, Unified Joint Task List

5.14 Development of Cyber Theory

- What is the foundation of cyber theory?
- What USAF doctrine exists pertaining to cyber warfare?
- What is the recommended composition of a cyber force?
- What is the recommended organization and composition of such a force? Should the force be primarily offensive or defensive?
- Can/should the USAF shape the cyber environment?

POC: INSS, 719-333-2717/DSN 333-2717, Dr. Chris Cain 334-953-1028.
Priority: 2
Key Terms: Information Operations, law, policy

5.15 Cyber Attack Case Studies

- What were the potential types of responses to recent case of cyber warfare (e.g., Estonia incident, Chinese "Titan Rain" cyber attack, etc)?
- What are the sovereignty issues involved?
- Were these attacks or any other cyber attacks considered a sovereignty violation or an attack? What are the threshold limits?
- Do such attacks warrant a like response or a military response? What is the proper response?

POC: INSS, 719-333-2717/DSN 333-2717, Dr. Kuehl, NDU, 202-685-2257
Priority: 2
Key Terms: Information Operations, law, policy

5.16 The role of IO in counterinsurgency or counterterrorism operations

- Discuss how IO can be used to reduce the effectiveness of insurgency or terrorist operations.
- What are some steps the US might take from a policy perspective?
- How can IO be used to dissuade the origins of insurgency?
- Who is the target audience for short term and long term counterinsurgency/counterterrorism IO strategies?
- How do insurgent or terrorist groups leverage IO and technology and what can be done to counter their strategies?
- Describe ways the US might respond to propaganda and hostile media.

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 2
Key Terms: Information Operations, insurgency, terrorism, influence, policy

5.17 How can we improve IO in a coalition/allied environment?

- How do security concerns and improved technologies impact IO in a coalition/allied environment? What do/don't we share or disclose? How do we overcome these concerns? How does this issue relate to homeland defense?
- How do netcentric operations improve coalition/allied capabilities?
- Do current Concepts of Operations need to be changed? How?
- How have allies such as the UK or NATO handled IO better? Examine the concept of operations for allied Public Information Officers in relation to US Public Affairs Officers.
- Analyze real world and exercise examples of successes and failures of IO operating in a coalition/allied effort.

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 2
Key Terms: IO, IW, coalition, security, homeland defense

5.18 What lessons can be learned from the private sector regarding defensive IW?

- What are the similarities and differences in the challenge of protecting the information resources of globally dispersed operations?
- How does a large, geographically dispersed organization identify, protect, and defend its most critical information assets?
- What is the best mix of centralized/decentralized protection and reserve/backup paths and systems in defending the most critical information assets?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 2
Key Terms: IO, IW, defensive IW, lessons learned, private sector, commercial

5.19 Domestic strategic communications

- Many are of the opinion that Air Force is not as effective as the other Services in informing and advising political/civilian leadership.
- Is this statement true? If yes, identify reasons why the Air Force is not as effective and present suggestions to improve the Air Force's performance in that arena.

- If it is not true, explain why and how the Air Force is effective at informing and advising with regards to its own interest.
- How can the Air Force improve its ability to communicate the US's mission and the Air Force's role in that mission to the US population, political/civilian leadership, the other Services, and world?
- How should the Air Force communicate US policies and the Air Force's role in those policies?

POC: Dr. Kuehl., NDU, 202-685-2257
Priority: 2
Key Terms: influencing political process, Air Force communications, US policy, political/civilian leadership

5.20 Explore the concept of computer network exploitation (CNE)/"Active Defense"/responsive action.

- Define concept of CNE/"active defense" in cyber-warfare and how it is distinguished from related CND, Computer Network Attack (CNA), and Info Assurance activities.
- What advantages does having authorization and capability to conduct CNE/"active defense" as part of CND provide? What are the implications of not having authority?
- What policy and legal considerations apply to CNE/"active defense" and the establishment of ROE for its prosecution?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key Terms: IO, IW, CNE, active defense, legal, cyber-warfare

5.21 Analyze the requirements to establish organizations to conduct cyber warfare.

- Discuss the organizational requirements.
- Should a new Command be stood up? Which functions should be conducted
    - at the Joint, MAJCOM, NAF, and AOC levels?
- What tools do commanders need to conduct IO at each level (Service
    - component, JTF, Combatant Commander)?
- Identify the key skills and knowledge areas needed to establish a cyber
    - workforce
- Identify the key skills and knowledge areas every Airman should know about the cyber mission area
- Discuss the education and training requirements to build a cyber workforce.
- How should cyber expertise be managed?
- How integrated with the other IO disciplines (Influence and Electronic
    - Warfare Ops) should a cyber operator be?
- What are the potential roles for the Guard and the Reserve?

POC: INSS, 719-333-2717/DSN 333-2717
Priority: 3
Key Terms: Information Operations, Command and Control, education and training